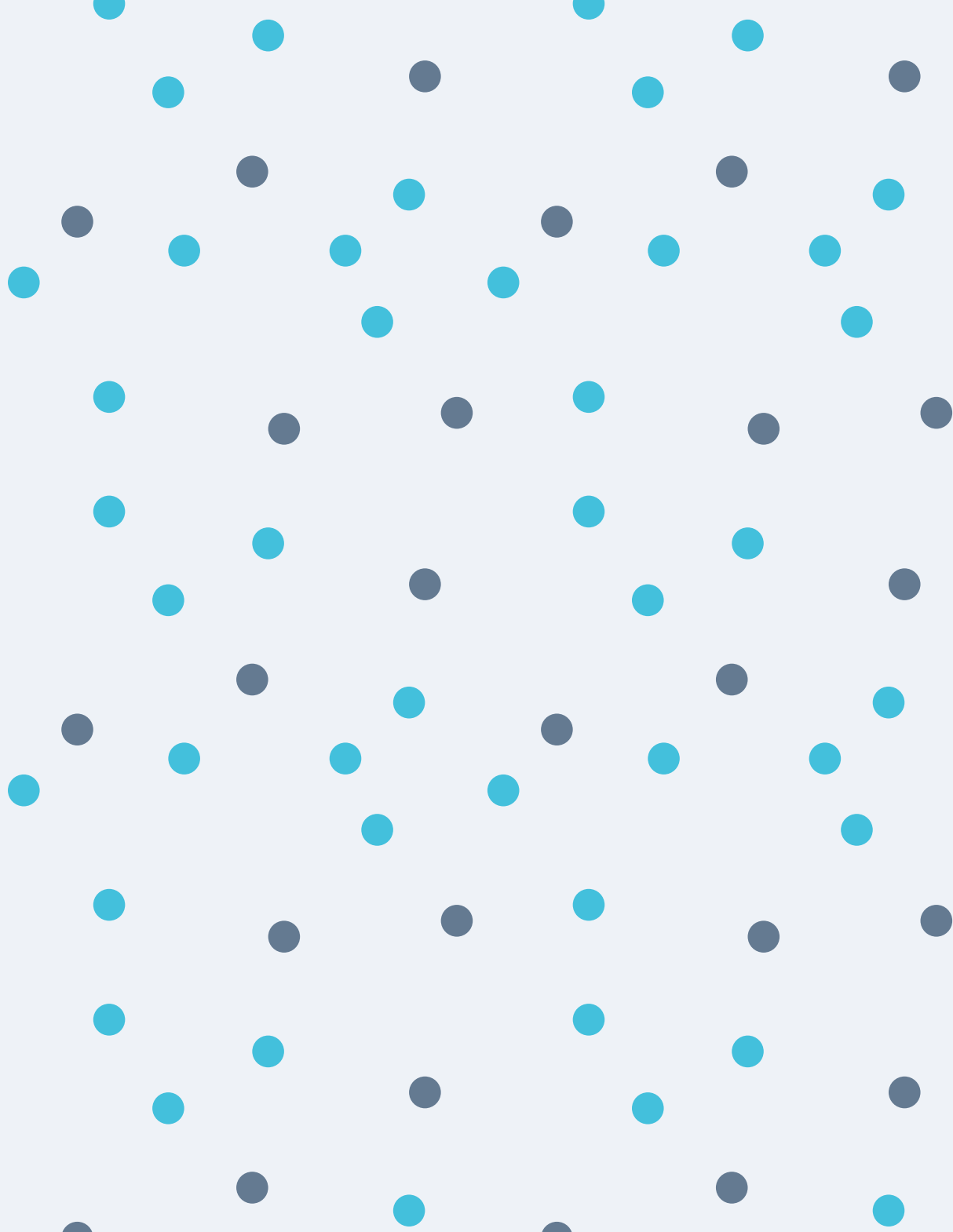


Math 136 Lecture Note

Exercise) find with proves, $n>1$, such that n^3-1 is prime

Solutions:

Let $n>1$ be an integer, assume that n^3-1 is prime

Since $n^3-1=(n-1)(n^2+n+1)$

Notice both are positive, we see that there are 2 options

$n-1=1$, $n-1=n^3-1$

Case 1: $n=2$, $n^3-1=7$ is prime

Case 2: $n^3=n \iff n^2=1 \iff n=\pm 1$ ← Cannot happen since $n>1$

Thus, $n=2$ is the only solution

Show sth is prime / composite → factor ⇒ one of them must be one

Concept review:

prime number

An integer $p>1$ is called prime $\iff$ its only positive divisor are 1 and p itself. Otherwise p is composite.

Note: 1 is not prime / composite

prime factorization

Every integer $n>1$ can be written as a product of primes.

Euclid's Theorem

There are infinitely many primes

Euclid's Lemma

For all integers a, b, and prime number p, if $p|ab$, then $p|a$ / $p|b$

Generalized Euclid's Lemma

Let p be a prime number, and let $a_1, a_2, \ldots a_n$ be integers.
If $p \mid (a_1 a_2 \cdots a_n)$, then $p \mid a_i$ for some $i \in \{1, 2, \ldots n\}$

Unique Factorization Theorem (UFT)

Every integer $n > 1$ can be written as a product of prime factors uniquely apart from the order of factors.

Proof:
We proceed by POSI on n

Base Case: If $n = 2$, then n is prime, only one ways.

Inductive Step:

Let $k \geq 2$, and assume that $2, 3, \ldots k$ has unique pf. We will show that $k+1$ also has upf. From pf, we know that pf say

$$k+1 = p_1 \cdots p_2 \cdot p_j.$$

Let $k+1 = q_1 \cdots q_2 \cdots q_e$ be another prime factorization of $k+1$.
Since $p_1 \mid (k+1)$, we have $p_1 \mid (q_1 q_2 \cdots q_e)$
Since p_1 is prime, it follows GEL that

$$p_1 \mid q_i \quad \text{for some } i \in \{1, 2, \ldots, l\}$$

Without loss of generality, May assume that $i = 1$. So $p_1 \mid q_1$, so they must equal
Thus $(k+1) = p_1 p_2 p_3 \cdots p_j$

$$= p_1 p_2 p_3 \cdots q_e$$

Now if $(k+1)$ is prime, then $(k+1) = p_1 = q_1$, so we're done.
If $(k+1)$ is composite, then for $m \frac{k+1}{p_1}$, we have

$$1 < m < k+1$$

And we have 2 pf of m:

$$m = p_2 p_3 \cdots p_j$$

$$= q_2 q_3 \cdots q_e$$

Since $2 \leq m \leq k$, the IH applies, so m has upf (order doesn't matter)

□

Finding a Prime Factor

$\forall n > 1$ (composite), $\exists$ prime $p \ni p \mid n$ and $p \leq \sqrt{n}$

Divisors from Prime Factorizations and the GCD

(Divisors From Prime Factorization (DFPF))

Let n and c be positive integers, and let

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

be a way to express n as a product of the distinct primes $p_1, p_2, \ldots, p_k$, where some or all of the exponents may be zero. The integer c is a positive divisor of n if and only if c can be represented as a product

$$c = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}, \text{ where } 0 \leq \beta_i \leq \alpha_i \text{ for } i = 1, 2, \ldots, k.$$

Math 135 Note

Oct 30

Congruent

Let m be a fixed positive integer. For integer a, b, we say that a is **congruent** to b modulo m, and write

$$a \equiv b \pmod{m}$$

when $m \mid (a-b)$. For integers a, b such that $m \nmid (a-b)$ we write $a \not\equiv b \pmod{m}$

$\equiv$ is congruence, and m is modulus

Properties of Congruence

1) Congruence is an Equivalence Relation (CER)

1. $\forall a, b, c \in \mathbb{Z}$, we have

a) $a \equiv a \pmod{m}$ b) if $a \equiv b \pmod{m}$ then $b \equiv a \pmod{m}$

c) $a \equiv b \pmod{m} \wedge b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$

① Since $a-a=0$, $m \mid 0$, $\therefore$ $a \equiv a \pmod{m}$

② Assume $a \equiv b \pmod{m}$ is true So $m \mid (a-b)$

Then $m \mid -(a-b)$ $[(a-b) \mid -(a-b)]$ by TD

So $m \mid (b-a)$, and $b \equiv a \pmod{m}$

③ Assume $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$

Then $m \mid (a-b)$ and $m \mid (b-c)$

by DIC, $m \mid ((a-b)x + (b-c)y)$ Let $x=1, y=1$

$m \mid (a-b+b-c)$

$m \mid (a-c)$

Thus, $a \equiv c \pmod{m}$

proposition 2

$\forall a_1, a_2, b_1, b_2 \in \mathbb{Z}, \left[(a_1 \equiv b_1 \pmod m) \wedge a_2 \equiv b_2 \pmod m \right] \Rightarrow$

1) $a_1 + a_2 \equiv b_1 + b_2 \pmod m$
2) $a_1 - a_2 \equiv b_1 + b_2 \pmod m$
3) $a_1 a_2 \equiv b_1 b_2 \pmod m$

Proof:

1) Assume $a_1 \equiv b_1 \pmod m$ and $a_2 \equiv b_2 \pmod m$ are true
then by DIC, $m \mid [(a_1 - b_1) + a_2 - b_2]$
$m \mid (a_1 + a_2) - (b_1 + b_2)$
So $a_1 + a_2 \equiv b_1 + b_2 \pmod m$

2) By DIC $m \mid a_1 - b_1 - (a_2 - b_2) = m \mid a_1 - a_2 - (b_1 - b_2)$
then $a_1 - a_2 \equiv b_1 - b_2 \pmod m$

3) By DIC $m \mid (a_1 - b_1)(a_2) + (b_1)(a_2 - b_2) = m \mid a_1 a_2 - b_1 b_2$
then $a_1 a_2 \equiv b_1 b_2 \pmod m$

Special Cases of proposition 2

$a_1 \equiv a_2 \pmod m$ is true, $b_1 \equiv b \pmod m$ (we can add, subtract, multiply by a constant on both sides)

1) $a_1 + b \equiv a_2 + b \pmod m$ 2) $a_1 - b \equiv a_2 - b \pmod m$
3) $a_1 b \equiv a_2 b \pmod m$

* replace a value by something if is congruent to a sum / difference / multiplication

Congruence Add and Multiply (CAM) (also subtraction)

$\forall n \in \mathbb{N}$, $\forall a_1 \ldots a_n \in \mathbb{Z}$, and $\forall b_1 \ldots b_n \in \mathbb{Z}$,
$\forall 1 \le i \le n$, $a_i \equiv b_i \pmod m \Rightarrow$

1) $a_1 + a_2 \ldots + a_n \equiv b_1 + b_2 + \ldots + b_n \pmod m$
2) $a_1 a_2 \ldots a_n \equiv b_1 b_2 \ldots b_n \pmod m$ ⟩ special case
3) $a^n \equiv b^n \pmod m$ Congruence Power Rule

Ex)

is $5^9 + 62^{2000} - 14$ divisible by 7?

Need to check if $5^9 + 62^{2000} - 14 \equiv 0 \pmod 7$

Note: $62 \equiv -1 \pmod 7$, $-14 \equiv 0 \pmod 7$, $5^2 \equiv 4 \pmod 7$, $4^2 \equiv 2 \pmod 7$

So by CAM, $5^9 + 62^{2000} - 14 \equiv (5^2)^4 \cdot 5 + (-1)^{2000} - 0 \pmod 7$

$\equiv 4^4 (5) + 1 - 0 \pmod 7$

$\equiv (4^2)^2 (5) + 1 \pmod 7$

$\equiv 2^2 (5) + 1 \pmod 7$

$\equiv 21 \pmod 7$

$\equiv 0 \pmod 7$

Thus, by CAM, we prove that $5^9 + 62^{2000} - 14$ is divisible by 7

Division?

Check: $3 \equiv 24 \pmod 7$ (both are divisible 3) Sometimes Division Works

$1 \equiv 8 \pmod 7$ also $3 \equiv 27 \pmod 6$

$1 \not\equiv 9 \pmod 6$

* when Common Divisor and m are coprime, then Division Works.

Congruence Divide CD

$\forall a, b, c \in \mathbb{Z}$, if $ac \equiv bc \pmod m$ and $\gcd(c, m) \equiv 1$ then $a \equiv b \pmod m$

Proof:

Let $a, b, c \in \mathbb{Z}$. Assume $ac \equiv bc \pmod m$ and $\gcd(c, m) \equiv 1$

Then $m \mid ac - bc$ and $m \mid c(a-b)$

Since $\gcd(c, m) = 1$, then by CAD $m \mid a - b$

So, $a \equiv b \pmod m$

Multiply a constant is not reversible.

Ex) $x \in \mathbb{Z}$. then $-5x \equiv -5(2^{2022}) + 5^{135} - 50 \pmod 9$

By inspection $\gcd(-5, 9) = 1$, then

$x \equiv 2^{2022} - 5^{134} + 10 \pmod 9$

Note that $10 \equiv 1 \pmod 9$ $2^3 \equiv 1 \pmod 9$ $5^3 \equiv -1 \pmod 9$ $5^2 \equiv 7 \pmod 9$

$x \equiv (2^3)^{674} - (5^3)^{44} \cdot 5^2 + 1 \pmod 9$

$x \equiv (-1)^{674} - (-1)^{44} \cdot 25 + 1 \pmod 9$

$x \equiv 1 - 24 + 1 \pmod 9$

$x \equiv 1 - 7 + 1 \pmod 9$

$x \equiv -5 \pmod 9$

$x \equiv 4 \pmod 9$

$\therefore x \equiv 4$

November 1st.

Lemma. *Fix $m \in \mathbb{N}$. Every integer is congruent (mod m) to its remainder when it is divided by m.*
Proof sketch.

Proof:

Let $a \in \mathbb{Z}$, Let q, r be the quotient and remainder when a is divided by m

then $a = qm + r$, $0 \le r < m$

$a - r = qm$

$m \mid a - r$

then by Definition, $a \equiv r \pmod m$

□

Congruent to Remainder (CTR) *Fix $m \in \mathbb{N}$. For all $a \in \mathbb{Z}$ and $r \in \{0, 1, \ldots, m-1\}$,*

$a \equiv r \pmod m \iff r$ *is the remainder when a is divided by m.*

Backward ⇐ Already proved

Forward ⇒ Contrapositive

Proof hint. The new ingredient is ($\implies$). Assume $r \in \{0, 1, \ldots, m-1\}$ and $a \equiv r \pmod m$. Let r_1 be the remainder when a is divided by m. Then $a \equiv r_1 \pmod m$ (by the Lemma). So $r \equiv r_1 \pmod m$ by (CER), which means $\boxed{m \mid (r - r_1)}$. But

$$0 \le r < m$$
$$-m < -r_1 \le 0$$

so adding gives

$$\boxed{-m < r - r_1 < m.}$$

The two boxed facts imply $r - r_1 = 0$, so $r = r_1$. □

Here is a different, but essentially equivalent, way of saying (CTR).

Congruent Iff Same Remainder (CISR) *Fix $m \in \mathbb{N}$. For all $a, b \in \mathbb{Z}$, $a \equiv b \pmod{m} \iff$ a and b have the same remainder when divided by m.*

(m | (a-b) = a, b have same remainder)

Ex) $m=5$ $a \equiv 121$ $b \equiv 36$ both a, b have $r=1$ when divided by 5

So $121 \equiv 36 \pmod 5$

Check: $121-36=85$, $5 | 85$

Example:

1) What is the remainder when $a = 77^{100} \cdot 999 - 6^{83}$ is divided by 4.

① Strategy: find $r \in \{0,1,2,3\} \ni a \equiv r \pmod 4$

Then by CIR, r = remainder

Note that $77 \equiv 1 \pmod 4$ $999 \equiv (-1) \pmod 4$ $6^2 \equiv 0 \pmod 4$

then $a \equiv (1)^{100} \cdot (-1) - (6^2)^6 \cdot 6^{19}$

$\equiv (1)^{100} \cdot (-1) - (0)^6 \cdot 6^{19}$ Note: Symplifying base

$\equiv -1 - 0$

$\equiv -1 \pmod 4$

$\equiv 3 \pmod 4$

$\therefore r = 3$ by CIR

Ex): $3 | 123$

Proposition 8. *For all $a \in \mathbb{N} \cup \{0\}$,* Non-negative ℤ

$$3 \mid a \iff 3 \mid (\text{the sum of the digits in the base-10 representation of } a).$$

Proof. Let $d_k d_{k-1} \cdots d_2 d_1 d_0$ be the base-10 representation of a. This means $d_0, d_1, \ldots, d_k \in \{0, 1, \ldots, 9\}$ and

$$a = d_k 10^k + d_{k-1} 10^{k-1} + \cdots + d_2 10^2 + d_1 10 + d_0.$$

Let S be the sum of the digits, i.e., $S = d_k + \cdots + d_2 + d_0$.

Observe that $10 \equiv 1 \pmod 3$. So by (CP), $10^n \equiv 1^n \pmod 3$ for any $n \geq 1$, i.e., $10^n \equiv 1 \pmod 3$. Because $\equiv$ plays nicely with sums and products (CAM), we can write

$$\begin{aligned} a &= d_k 10^k + d_{k-1} 10^{k-1} + \cdots + d_2 10^2 + d_1 10 + d_0 \\ &\equiv d_k(1) + d_{k-1}(1) + \cdots + d_2(1) + d_1(1) + d_0 \pmod 3 \\ &= S. \end{aligned}$$

Thus $a \equiv S \pmod 3$. So by (CISR), a and S have the same remainder when divided by 3. In particular, one has remainder 0 iff the other has remainder 0. □

There is a similar test for divisibility by 9, using the fact that $10 \equiv 1 \pmod 9$.

There is also a test for divisibility by 11.

Proposition 9. *For all $a \in \mathbb{N} \cup \{0\}$ with base-10 representation $d_k d_{k-1} \cdots d_2 d_1 d_0$,*

$$11 \mid a \iff 11 \mid (d_0 - d_1 + d_2 - \cdots + (-1)^{k-1} d_{k-1} + (-1)^k d_k).$$

Proof idea. $10 \equiv -1 \pmod{11}$, so $10^n \equiv (-1)^n \pmod{11}$ for each $n \geq 1$. □

November 3rd 8.4 8.5

Definition. A **linear congruence** (in one variable) is a congruence of the form

$$ax \equiv c \pmod{m}$$

where $m \in \mathbb{N}$ and $a, b \in \mathbb{Z}$ are fixed, and we seek solutions $x \in \mathbb{Z}$.

$m \mid ax - c$

a fixed

Ex) $2x \equiv 3 \pmod 5 \to x = 4$ $(2\cdot 4 - 3) = 5(1)$ $x = -1$ $(2\cdot(-1) - 3) = 5(-1)$

$5 \mid 2x - 3$

Set of solutions (list ... -11, -6, -1, 4, 9, 14, 19 ...)

$= \{ x \in \mathbb{Z},\ x \equiv 4 \pmod 5 \}$

3. $4x \equiv 5 \pmod{10}$ (No solution)

↳ $4x - 5$ is always odd

So can't have $10 \mid 4x - 5$

2. $2x \equiv 6 \pmod{10} \to x = 8,\ x = 18,\ x = 13,\ x = -2$

Solution set:

$\{ \ldots -12, -7, -2, 3, 8, 13, 18 \ldots \}$

$\{ x \in \mathbb{Z},\ x \equiv 3 \pmod 5 \}$

$\{ x \in \mathbb{Z},\ x \equiv 3 \text{ or } 8 \pmod{10} \}$

In general, consider $ax \equiv c \pmod m$

If $x \in \mathbb{Z}$, x is a solution to $\uparrow$ $\iff$ $m \mid ax - c$

$\iff$ $ax - c = mt$ (for some $t \in \mathbb{Z}$)

$\iff$ $ax - mt = c$ for some $t \in \mathbb{Z}$

$\iff$ $ax + my = c$ for some $t \in \mathbb{Z}$

So the solution to $ax \equiv c \pmod m$ = "x part" of the solution to $ax + my = c$

(LC) has a solution $\iff$ (LDE) has a solution $\iff$ $\gcd(a, m) \mid c$

If x_0 is 1 solution to (LC), the the general solution:

$x = x_0 + \frac{m}{d} k$ $k \in \mathbb{Z}$ (No need to worry about y)

$\frac{m}{d} \mid x - x_0 \implies x \equiv x_0 \pmod{\frac{m}{d}}$

So the solution set is $\{ x \in \mathbb{Z},\ x \equiv x_0 \pmod{\frac{m}{d}} \}$

Linear Congruence Theorem (LCT). *Fix $m \in \mathbb{N}$. For all $a, c \in \mathbb{Z}$ with $a \neq 0$, the linear congruence*

$$ax \equiv c \pmod m$$

has a solution iff $d \mid c$ where $d = \gcd(a, m)$. Moreover, if x_0 is one solution, then the full solution set is

$$\{x \in \mathbb{Z} : x \equiv x_0 \pmod{\tfrac{m}{d}}\}.$$

Equivalently, the solution set can be written in $(\bmod m)$ terms as

$$\{x \in \mathbb{Z} : x \equiv x_0 \text{ or } x_0 + \tfrac{m}{d} \text{ or } x_0 + 2\tfrac{m}{d} \text{ or } \ldots \text{ or } x_0 + (d-1)\tfrac{m}{d} \pmod m\}.$$

(d options)

proof of this

Ex) $15x \equiv 6 \pmod{21}$ Note that $\gcd(15, 6) = 3$, $3 \mid 6$. Solution exists.

one solution: by inspection / find a solution using EEA

$\swarrow x = -1$

EEA: $15x + 21y = 3$

1	0	21	0
0	1	15	0
1	−1	6	1
−2	3	3	2

By EEA, $(21)(-2) + (15)(3) = 3 \rightarrow x_0 = 3 \quad y_0 = -2$

Multiply by 2. $x_1 = 6 \cdot y_1 = -4$

then $15(6) + 21(-4) = 6$

So $x_1 = 6$ should be a soln to $15x \equiv 6 \pmod{21}$

$m/d = 7$

Full solution set: $\{x \in \mathbb{Z},\ x \equiv 6 \pmod 7\} = \{x \in \mathbb{Z},\ x \equiv 6 \text{ or } 13 \text{ or } 20 \pmod{21}\}$

Note: write all the solution sets $(0 \le x < m-1)$

Non-linear - Congruence (Non-linear polynomial Congruence)

Ex) $x^3 + 2x \equiv 3 \pmod{10}$

(No theorem) check each $x \in 0, 1, 2 \ldots 9$

$x \pmod{10}$	0	1	2	3	4	5	6	7	8	9
$x^2 \pmod{10}$	0	1	4	9	6	5	6	9	4	1
$x^3 \pmod{10}$	0	1	8	7	4	5	6	3	2	9
$x^3 + 2x \pmod{10}$	0	3	2	3	2	5	8	7	8	7

If x_1 is a solution, i.e. $x_1^3 + 2x_1 \equiv 3 \pmod{10}$, then $x_2 \equiv x_1 \pmod{10}$

then $x_2^3 + x_2 \equiv x_1^3 + 2x_1 \pmod{10}$

$\equiv 3 \pmod{10}$

Full solution set: $\{x \in \mathbb{Z},\ x \equiv 1, 3 \pmod{10}\}$

November 6th

$\equiv \pmod m$ is a useful relation on $\mathbb{Z}$, but sometimes we wish we could treat it as if it were just $=$. One way to do this is to construct a new number system.

Congruence class = a set of integer = name in indefinitely many ways.

Definition. Fix $m \in \mathbb{N}$. Given $a \in \mathbb{Z}$, the **congruence class modulo** m of a is the set

$$[a] = \{x \in \mathbb{Z} : x \equiv a \pmod{m}\}.$$

↑ square brackets

Ex) Fix $m=5 \Rightarrow [0] = \{x \in \mathbb{Z},\ x \equiv 0 \pmod 5\} = \{\ldots, -10, -5, 0, 5, 10\}$

$[1] = \{x \in \mathbb{Z},\ x \equiv 1 \pmod 5\} = \{\ldots -9, -4, 1, 6, \ldots\}$

Same as $[2], [3], [4]$ (all other sets are equal to those) $\{[5] = [0]\}$

Complication: Congruence classes can be named in more than one way (like fraction)

Rules for same name: $a/b = c/d = [ad = bc]$

Congruence classes (mod m) $[a] = [b] \iff a \equiv b \pmod m$

Definition. Fix $m \in \mathbb{N}$. We define $\mathbb{Z}_m$ (the set of congruent class (mod m)) to be the set $\{[0], [1], [2], \ldots, [m-1]\}$ and call it **the set of integers mod** m. We define **addition** and **multiplication** on $\mathbb{Z}_m$ by

$$[a] + [b] = [a + b]$$
$$[a] \cdot [b] = [ab].$$

(defined)

(Technically, we are *overloading notation*.) We call $+$ and $\times$ in $\mathbb{Z}_m$ **modular arithmetic**. It has most of the same properties as ordinary arithmetic, including:

Example) in $\mathbb{Z}_{12}$, $[9] + [5] = [2]$ $\qquad [9][5] = [45] = [9]$

Calculation: $[9] + [5] = [9+5] = [14] = [2]$ $\qquad [45] \equiv 9 \pmod{12}$

Arithmetic in $\mathbb{Z}_m$:

properties:

① $[a] + [b] = [b] + [a]$ ② $[0] + [0] = [0]$ ③ $[a] + [-a] = 0$

④ $[a] \cdot [b] = [b] \cdot [a]$ ⑤ $[a] \cdot [1] = [a]$

Commutative for ⊕ $[0]$ is an additive identity

Commutative for ⊗ $[1]$ is a multiplicative identity

Every $[a]$ has an **additive inverse**

Modular Arithmetic Theorem (MAT) *Fix $m \in \mathbb{N}$. Given $a, c \in \mathbb{Z}$, the equation*

$$[a][x] = [c]$$

has a solution in $\mathbb{Z}_m$ $\iff$ $d \mid c$ where $d = \gcd(a, m)$. When solutions exist, there are exactly d distinct solutions:

$$[x_0],\ [x_0 + \tfrac{m}{d}],\ [x_0 + 2\tfrac{m}{d}], \ldots, [x_0 + (d-1)\tfrac{m}{d}]$$

where $[x_0]$ is one particular solution.

Ex) In $\mathbb{Z}_{10}$, solve $[12][x]+[3]=[8]$

Solutions: $[2][x] = [5]$ $\quad m=10$

$d = \gcd(2,10) = 2$, $2 \nmid 5$ So by MAT, there's no solutions

Ex) In $\mathbb{Z}_{15}$, solve $[25][x]-[3]=[7]$

Solve: $[10][x] = [10] \Rightarrow [1][x]=[10]$

By MAT, $d = \gcd(10,15) = 5$ then $5 \mid 10$ checked

We will get 5 solutions $(d=5)$

$[x_0]=[1]$, is a particular solution, So the solution set is:

$[1], [4], [7], [10], [13]$

Proof:

for $[b] \in \mathbb{Z}_m$, $[b]$ is a soln to $[a][x]=[c] \Leftrightarrow b$ is a solution to $ax \equiv c \pmod m$

LCT gives solution

Additive Inverse

In $\mathbb{Z}_5$, $[2]\cdot[3]=[1]$, so $[2]^{-1} = [3]$ (additive reverse)

Mult. Inverse

If $[a]\cdot[b]=[1]$, then $[b]$ is called the mult. inverse of $[a]$

Notation: $[b]=[a]^{-1}$

In $\mathbb{Z}_6$: $[1]^{-1}=[1]$ $\quad [2]^{-1}=[3]$ $\quad [3]^{-1}[2]$ $\quad [4]^{-1}[4]$

Inverses in $\mathbb{Z}_m$ (INV $\mathbb{Z}_m$) *Fix $m \in \mathbb{N}$. An element $[a]$ in $\mathbb{Z}_m \setminus \{[0]\}$ has a multiplicative inverse $\iff$ $\gcd(a, m) = 1$. Moreover, when $[a]^{-1}$ exists, it is unique.*

$[a]^{-1}$ exists $\Leftrightarrow [a]\cdot[x]=[1]$ has a solution in $\mathbb{Z}_m$

Corollary (Inverses in $\mathbb{Z}_p$ (INV $\mathbb{Z}_p$)). *For every prime p, every nonzero element in $\mathbb{Z}_p$ has a multiplicative inverse.*

November 8th

Why care Multiplicative Inverse:

In equations over $\mathbb{Z}_m$, can't divided by $[a]$

$[a][b] = [a][c] \not\Rightarrow [b] = [c]$

Example: $[6][2] = [10] = 0 \pmod{10}$

$[6][4] = [20] = 0 \pmod{10}$

$b \neq c$

$\Rightarrow$

However if $[a]^{-1}$ exists, by multiply $[a]^{-1}$:

$[a][b] = [a][c] \Rightarrow [a]^{-1}[a][b] = [a]^{-1}[a][c]$

$\Rightarrow [b] = [c]$

Special Cases => when m is prime, every $a = 1, 2 \ldots m-1$ is coprime to m

Inverses in $\mathbb{Z}_p$ (INV $\mathbb{Z}_p$)

Fix a prime p. Every nonzero $[a] \in \mathbb{Z}_p$ has a multiplicative inverse $[a]^{-1}$.

8.7

Exercise) Reduce $2^6 \pmod 7 \equiv 1 \pmod 7$

$3^6 \pmod 7 \equiv 8 \pmod 7$ By Congruence Power

$\equiv 1 \pmod 7$ By Transibility

Reduce $4^6 \pmod 7 \equiv 2 \pmod 7 \Rightarrow 1 \pmod 7$

Note: $4^3 \equiv 2 \pmod 7$

Fermat's Little Theorem (FℓT)

$\forall$ primes p, $\forall a \in \mathbb{Z}$ with $p \nmid a$,

$$a^{p-1} \equiv 1 \pmod p.$$

Sample Application

① Find the remainder when 12^{95} is divided 7 By CTR

Solution:

7 is prime and $7 \nmid 12$. By FLT, $12^6 \equiv 1 \bmod 7$

Since $(12^6)^{15} \equiv 1^{15} \pmod 7$ By CP

So $12^{90} \cdot 12^2 \equiv 1 \cdot 12^2 \pmod 7$ By CAM, CP

$\equiv 5^2 \pmod 7 \equiv 4 \pmod 7$ So remainder is 4 by CTR

Find $[5]^{-1}$ in $\mathbb{Z}_7$

Solution:

By inspection, $[5]^{-1} = [3] \Leftarrow [15] = 1 \pmod 7$

7 is prime, $7 \nmid 5$, so by FLT, $5^6 \equiv 1 \pmod 7$. $\equiv [5]^6 = [1]$ in $\mathbb{Z}_7$

So $[5]\cdot[5]^5 = [1] \Rightarrow [5]^{-1} = [5]^5 \Rightarrow [-2]^5 = [-2]^3\cdot[-2]^2 = [-1]\cdot[4] = [3]$

Proof of FLT:

Proof of (FℓT) Strategy: use the arithmetic of $\mathbb{Z}_p$.

Given: prime p, $a \in \mathbb{Z}$ with $p \nmid a$.

So $a \not\equiv 0 \pmod p$. So $[a] \neq [0]$ (in $\mathbb{Z}_p$).

Look at

$$[a],\ [2a],\ [3a],\ \ldots,\ [(p-1)a] \qquad (*)$$

Claim 1. Every $[ka]$ in this list is nonzero.

Proof: Suppose $\exists\, k \in \{1,2,\ldots,p-1\}$ with $[ka] = [0]$.
Then $ka \equiv 0 \pmod p$, so $p \mid ka$, so $p \mid k$ or $p \mid a$. (EL)
But $p \nmid k$ and $p \nmid a$. (Contradiction) (Every $[ka]$ is >0)

Claim 2. The $p-1$ elements in the list are all distinct. (unique)

Proof: Suppose $\exists\, i, k \in \{1,2,\ldots,p-1\}$ with $i \neq k$, and yet $[ia] = [ka]$.
Write this as $[i][a] = [k][a]$. By (INV $\mathbb{Z}_p$), $[a]^{-1}$ exists.
So $[i][a][a]^{-1} = [k][a][a]^{-1}$ which simplifies to $[i] = [k]$.
But $[i] \neq [k]$. (Contradiction) Proof continues on next page

Proof (continued)

$$[a],\ [2a],\ [3a],\ \ldots,\ [(p-1)a] \qquad (*)$$

Claim 1. Every $[ka]$ in this list is a nonzero element of $\mathbb{Z}_p$.

Claim 2. The $p-1$ elements in the list are all distinct.

Conclusion: the list $(*)$ is just $[1], [2], [3], \ldots, [p-1]$, but rearranged.

Example: if $p = 7$ and $a = 4$,

$$[4],\ [2(4)],\ [3(4)],\ [4(4)],\ [5(4)],\ [6(4)] \qquad (*)$$

is

$$[4],\ [1],\ [5],\ [2],\ [6],\ [3] \quad \text{(rearrange)}$$

Proof (continued)

So $$\boxed{[a]\cdot[2a]\cdot[3a]\cdots[(p-1)a] = [1]\cdot[2]\cdot[3]\cdots[p-1].}$$

(product, product) (Proof continues on next page)

Proof (continued).

$$[a]\,[2a]\,[3a]\cdots[(p-1)a] = [1]\,[2]\,[3]\cdots[p-1].$$

Rewrite:

$$[a]\,\big([2]\,[a]\big)\,\big([3]\,[a]\big)\cdots\big([p-1]\,[a]\big) = [1]\,[2]\,[3]\cdots[p-1].$$

Rearrange:

$$\boxed{\big([2]\,[3]\cdots[p-1]\big)\,[a]^{p-1} = \big([2]\,[3]\cdots[p-1]\big)\,[1].} \qquad (\dagger)$$

p is prime. By (INV $\mathbb{Z}_p$), $[k]^{-1}$ exists for each $k = 2, 3, \ldots, p-1$.

So we can multiply both sides of $(\dagger)$ by $[2]^{-1}$, then $[3]^{-1}$, etc. to get

$$[a]^{p-1} = [1] \quad \text{(in } \mathbb{Z}_p\text{)},$$

which means $$a^{p-1} \equiv 1 \pmod p.$$ □

Another Application:

Corollary 15

$\forall$ primes p, $\forall\, a \in \mathbb{Z}$,

$$a^p \equiv a \pmod p.$$

Proof:

Suppose p is prime and $a \in \mathbb{Z}$.

- If $p \nmid a$, then $a^{p-1} \equiv 1 \pmod p$ by (FℓT). So $a^p \equiv a \pmod p$.
- If $p \mid a$, then $a \equiv 0 \pmod p$ so

$$a^{p-1} \equiv 0^{p-1} = 0 \pmod p \quad \text{and} \quad a^p \equiv 0 \pmod p.$$

In both cases,

$$a^p \equiv a \pmod p.$$

Ex) $a^{107} \pmod 7$

Solution:

By CRT6, $a^7 = a \pmod 7 \Rightarrow (a^7)^{15}\cdot a^2 \equiv a^{15}\cdot a^2 = a^{17} \pmod 7$

Further: $(a^7)^2\cdot a^3 = a^2\cdot a^3 = a^5 \pmod 7$ So $a^{107} \equiv a^5 \pmod 7$ $\forall a \in \mathbb{Z}$

November 8th

Exercise) Find all integer solution $x \in \mathbb{Z}$ satisfying $x \equiv 2 \pmod{13}$, $x \equiv 7 \pmod{29}$

Solution:

① Solve $x \equiv 2 \pmod{13} \Rightarrow x \equiv 2 + 13n \ (n \in \mathbb{Z})$

Sub $(x \equiv 2 + 13n \ (n \in \mathbb{Z}))$ to $x \equiv 7 \pmod{29} \Rightarrow 2 + 13n \equiv 7 \pmod{29}$

$13n \equiv 15 \pmod{29}$ Since $\gcd(15, 29) = 1$ and $1 \mid 5$ By LCT, n_0 is one solution

Need one solution n_0 to $13n \equiv 15 \pmod{29} \Rightarrow 13n + 29y = 15$

1	0	29	0
0	1	13	0
1	-2	3	2
-4	9	1	4

then by EEA, $n = 9$, $y = -4$

Multiply by 15 $\Rightarrow n_0 = 135$ is a particular solution to $13n \equiv 15 \pmod{29}$

Simplifying, we get $n \equiv 19 \pmod{29} \Rightarrow n = 19 + 29k \ (k \in \mathbb{Z})$

Sub into 1. then $x = 2 + 13(19 + 29k) \Rightarrow \boxed{x = 249 + 377k}$ ← actual Solution

Change to congruence expression

Full solution set is all $x \in \mathbb{Z}$ such that $x \equiv 249 \pmod{377}$

Notice: $\gcd(13, 29) = 1$

Chinese Remainder Theorem

Chinese Remainder Theorem (CRT)[1] *For all $a_1, a_2 \in \mathbb{Z}$ and $m_1, m_2 \in \mathbb{N}$, if $\gcd(m_1, m_2) = 1$ then the system*

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$

has a unique solution (mod $m_1 m_2$). Thus if x_0 is one solution, then the full solution is given by

$$x \equiv x_0 \pmod{m_1 m_2}.$$

Proof. Read in the course notes if interested. □

Example) $\begin{cases} n \equiv 2 \pmod{3} \\ n \equiv 3 \pmod{5} \end{cases}$ by inspection: $n = 8$ by CRT $\Rightarrow \{ n \equiv 8 \pmod{15} \}$

Example) $\begin{cases} x \equiv 4 \pmod{7} \\ x \equiv 5 \pmod{11} \end{cases}$ $\gcd(7, 11) = 1$, so CRT can be applied

① Start with larger mod ($x \equiv 5 \pmod{11}$ in this way) and write as an equation

$x = 5 + 11n \ (n \in \mathbb{Z})$

② Replace another congruence with ↑ equation and simplify

$6+11n \equiv 4 \pmod 7 \Rightarrow 4n \equiv -1 \pmod 7$

By LCT, if we have one solution, the the full solution is $n \equiv n_0 \pmod 7$

By Inspection, $n=5$ is a particular solution to $4n \equiv -1 \pmod 7$ ← Solution

By LCT. and $\gcd(4,11)=1$. The complete solution is: $n \equiv 5 \pmod 7 \Rightarrow n = 5+7k\ (k \in \mathbb{Z})$

③ Put ② solution back to the ① equation

$X = 5 + 11(5+7k) \Rightarrow X = 60+77k\ (k \in \mathbb{Z}) \Rightarrow X \equiv 60 \pmod{77}$

Solve
$$\begin{cases} X \equiv 5 \pmod 6 \\ X \equiv 2 \pmod 7 \\ X \equiv 3 \pmod{11} \end{cases}$$

By inspection, $x_0 = 23$ is one solution to first 2 congruence

By CRT, $X \equiv 23 \pmod{42}$ is a solution to first 2 congruence

---

November 12th

Generalized Chinese Remainder Theorem (GCRT) *For all $k, m_1, m_2, \ldots, m_k \in \mathbb{N}$ and $a_1, a_2, \ldots, a_k \in \mathbb{Z}$, if $\gcd(m_i, m_j) = 1$ for all $i \neq j$, then the system of simultaneous congruences*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

has a unique solution modulo $m_1 m_2 \cdots m_k$. Thus if x_0 is one solution, then the complete solution is

$$\{x \in \mathbb{Z} : x \equiv x_0 \pmod{m_1 m_2 \cdots m_k}\}.$$

Method: solve the first two congruences $\pmod{m_1}$ and $\pmod{m_2}$, replacing them with a congruence $\pmod{m_1 m_2}$. Then repeat.

Note: for this to work, the new modulus $m_1 m_2$ needs to be coprime to $m_3, \ldots, m_k$. This follows from

$$\forall a, b, c \in \mathbb{Z},\ \gcd(a,c) = \gcd(b,c) = 1 \implies \gcd(ab, c) = 1.$$

Example: $\begin{cases} 3X \equiv 2 \pmod 5 \\ 2X \equiv 6 \pmod 7 \end{cases} = \begin{matrix} X \equiv 4 \pmod 5 \\ X \equiv 3 \pmod 7 \end{matrix}$

Solution: look at each congruence separately:

① $3X \equiv 2 \pmod 5$

$\gcd(3,5) \equiv 1 \mid 12 \Rightarrow$ has a solution

Solution: $X \equiv X_0 \pmod 5 \Rightarrow X \equiv 4 \pmod 5$

② Same thing, $X=3$

Now: apply CRT, by inspection: $x_0 = 24$ is a particular solution $\Rightarrow$ By CRT $X \equiv 24 \pmod{35}$ is the full solution

Example: $\begin{cases} x \equiv 4 \pmod 6 \\ x \equiv 2 \pmod 8 \end{cases}$ ← Not coprime, so no CRT

from $x \equiv 2 \pmod 8$, write equation

↳ $x = 2 + 8n$ $(n \in \mathbb{Z})$ ⇒ $2 + 8n \equiv 4 \pmod 6$ ⇒ $8n \equiv 2$ or $2n \equiv 2 \pmod 6$] Find solution to one congruence

↳ By LCT, $\gcd(2,6) = 2$, $n_0 = 1$ is a solution, so full solution is $n \equiv 1 \pmod 3$]

↳ $n = 1 + 3k$ $(k \in \mathbb{Z})$ ⇒ $x = 2 + 8(1 + 3k)$ ⇒ $x = 10 + 24k$ ⇒ $x \equiv 10 \pmod{24}$] Sub to another

Splitting Modulus Theorem (SMT). *For all $m_1, m_2 \in \mathbb{N}$ and $a, b \in \mathbb{Z}$, if $\gcd(m_1, m_2) = 1$, then*

$$a \equiv b \pmod{m_1 m_2} \iff \begin{cases} a \equiv b \pmod{m_1} \\ a \equiv b \pmod{m_2}. \end{cases}$$

Example: $a \mid c$ ∧ $b \mid c$, $\gcd(a,b) = 1$ ⇒ $ab \mid c$

Solve $x^2 \equiv 5 \pmod{55}$

SOLUTION. By setting $a = x^2$, $b = 5$, $m_1 = 5$, and $m_2 = 11$ and noting that $\gcd(5, 11) = 1$, we get from (SMT) that

$$x^2 \equiv 5 \pmod{55} \iff \begin{cases} x^2 \equiv 5 \pmod 5 \\ x^2 \equiv 11 \pmod{11} \end{cases}$$

These are not linear congruences, but we can solve each one by brute force search:

$$x^2 \equiv 5 \pmod 5 \iff x^2 \equiv 0 \pmod 5$$

while

$$x^2 \equiv 5 \pmod{11} \iff x^2 \equiv 4 \text{ or } 7 \pmod{11}$$

Solution to $x^2 \equiv 5 \pmod{55}$ are $x \in \mathbb{Z}$ such that

⇐ $x \equiv 0 \pmod 5 \wedge x \equiv 4 \pmod{11}) \vee (x \equiv 7 \pmod{11})$

Rewrite: $[x \equiv 0 \pmod 5) \wedge (x \equiv 4 \pmod{11})] \vee [(x \equiv 0 \pmod 5) \wedge (x \equiv 7 \pmod{11})]$ by Distributive Law

Solve → By CRT

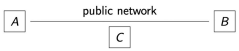
$x_0 \equiv 15 \pmod{55}$ by inspection or $x_0 \equiv 40 \pmod{55}$ by inspection

Full solution set:

$$\{x \equiv 15 \text{ or } 40 \pmod{55}\}$$

November 15th

Secure Communication



A sends a message to B like this:

- A translates the message to gibberish (**encryption**).
- The encrypted message is sent on the network.
- B translates the gibberish back to the original message (**decryption**)
- A and B use a standard protocol (known to all).
- A and B share a secret **key**.

Problem: how do A and B get their secret key?

- Circularity: can't securely communicate the key, unless a key has already been shared...

One key-pair protocol in use: RSA (= Rivest, Shamir and Adleman)

RSA exploits:

- relative ease of generating random large primes ($\approx$ 300-500 digits)
- practical impossibility of factoring products of random large primes.

To create a key pair using RSA, Bob will:

1. Randomly generate two (distinct) large primes p, q.
2. Multiply them to get $n = pq$.
3. Calculate the *Euler totient* $\phi(n) := (p-1)(q-1)$.
4. Randomly generate $e \in \mathbb{N}$ which is coprime to $(p-1)(q-1)$.
5. Find a solution $d \in \mathbb{N}$ to $ex \equiv 1 \pmod{(p-1)(q-1)}$.

Bob's public (encryption) key will be (e, n).

Bob's private (decryption) key will be (d, n).

From now on:

A = Alice $\qquad$ B = Bob

Alice wants to send a message to Bob.

Their shared key has two functions:

- For Alice: to encrypt the message to gibberish.
- For Bob: to decrypt the gibberish back to the message.

Alice only needs the encryption functionality.

Solution to the Circularity Problem: (resolved)

- Create separate (but paired) keys for encryption and decryption.
- Only send the encryption key over the network.

1. Bob creates two keys: one used for encryption, the other for decryption. They must be "inverse to each other."
2. Bob sends the encryption key to Alice (insecurely).
   - In fact, Bob posts the encryption key publicly on his webpage.
3. Alice uses Bob's encryption key to encrypt a message. The encrypted message is transmitted (insecurely) over the network.
4. Bob, and only Bob, has the decryption key. Bob can decrypt the message; no one else can.

Requirements:

- It must be easy for Bob to create (essentially random) key pairs.
- It must be essentially impossible for a supercomputer to deduce the decryption key from knowledge of the encryption key.

This scheme is a big part of the "public key certificates" standard (X.509) which forms the basis for HTTPS.

- p, q distinct primes
- $n = pq$
- $ed \equiv 1 \pmod{(p-1)(q-1)}$ and $1 < d, e < (p-1)(q-1)$

Bob's public (encryption) key: (e, n)

Bob's private (decryption) key: (d, n)

RSA protocol for encryption/decryption: raising to powers $\pmod n$

- Message: must be an integer M such that $0 \le M < n$.
- To encrypt M, Alice calculates $M^e \pmod n$. That is:
  - Alice finds C such that $0 \le C < n$ and $M^e \equiv C \pmod n$.
- To decrypt C, Bob calculates $C^d \pmod n$. That is:
  - Bob finds R such that $0 \le R < n$ and $C^d \equiv R \pmod n$. $\qquad R = M$

Example: network security at Western

Suppose Bob chooses

$p = 7$ (large prime)

$q = 13$ (different large prime)

$n = pq = 91$

$(p-1)(q-1) = 72$

$e = 5$ $\qquad \gcd(e, 72) = 1$, $1 < e < 72$

(between 1 and $(p-1)(q-1)$)

Bob then solves

$5x \equiv 1 \pmod{72} \Rightarrow x = 29 \pmod{72}$

and gets

$d = 29$ $\qquad 1 < d < 72$

Bob's public (encryption) key: $(e, n) = (5, 91)$

Bob's private (decryption) key: $(d, n) = (29, 91)$

$2x \equiv 1 \pmod{2 \cdot 36}$.

Bob's public (encryption) key: $(e, n) = (5, 91)$

Bob's private (decryption) key: $(d, n) = (29, 91)$

The world (including Alice) knows Bob's public key $(5, 91)$.

Alice composes her message M with $0 \le M < 91$. Say $M = 10$.

To encrypt this message, Alice must compute $10^5 \equiv C \pmod{91}$, $0 \le C < 91$. (M^e)

$$100000 \div 91 = 1098 \text{ with remainder } 82.$$

$$\therefore \quad 10^5 \equiv 82 \pmod{91}$$

The encrypted message is

$$C = 82.$$

Alice transmits the message "82" to Bob over the network.

Bob's private (decryption) key: $(29, 91)$

Bob is delivered the encrypted message "82." (decryption key d)

To decrypt this message, Bob computes $82^{29} \equiv R \pmod{91}$, $0 \le R < 91$.

82^{29} is a big number. Bob doesn't actually compute it; he just needs to figure out what it is congruent to mod 91.

- In real life, Bob pulls up an online calculator, such as the one at
  `https://www.omnicalculator.com/math/power-modulo`
- On an exam, Bob notes that

$82 \equiv -9 \pmod{91}$ and so $82^2 \equiv (-9)^2 = 81 \equiv -10 \pmod{91}$

$82^4 = (82^2)^2 \equiv (-10)^2 = 100 \equiv 9 \pmod{91}$

$82^8 = (82^4)^2 \equiv 9^2 = 81 \equiv -10 \pmod{91}$

$82^{16} = (82^8)^2 \equiv (-10)^2 = \cdots \equiv 9 \pmod{91}$

$82^{24} = (82)^8 \cdot (82)^{16} \equiv (-10)(9) = -90 \equiv 1 \pmod{91}$

and so $82^{29} \equiv 82^5 = 82 \cdot 82^4 \equiv (-9)9 = -81 \equiv 10 \pmod{91}$. $R = 10$

Why does RSA work (part 1)?

In the example, the world knows Bob's public key $(e, n) = (5, 91)$.

The world also knows that $n = 91$ is a product of two primes p and q.

But 91 is so large that our computers can't factor it to find p and q.

So we can't calculate $(p-1)(q-1)$.

So we don't know the modulus of the LC of which d is a solution:

$$5x \equiv 1 \pmod{?}$$

So we can't find the decryption key $d = 29$.

Why does RSA work (part 2)?

I.e., why does raising to the power d "reverse" raising to the power e?

RSA Works (RSA) – short version

For all $p, q, n, e, d \in \mathbb{Z}$, if

1. p and q are primes with $p \neq q$,
2. $n = pq$,
3. $ed \equiv 1 \pmod{(p-1)(q-1)}$ ed both > 0

then for all $M \in \mathbb{Z}$, $(M^e)^d \equiv M \pmod{n}$.

Proof idea

The modulus factors as $n = pq$ where $\gcd(p, q) = 1$. So by (SMT),

$$M^{ed} \equiv M \pmod{n} \iff \begin{cases} M^{ed} \equiv M \pmod{p} \\ M^{ed} \equiv M \pmod{q} \end{cases}$$

We can establish the congruences on the right using (FℓT) and (3).

Proof (details)

$ed \equiv 1 \pmod{(p-1)(q-1)}$

Proof of $\boxed{M^{ed} \equiv M \pmod{p}}$ (Proof of $M^{ed} \equiv M \pmod{q}$ is similar.)

Case 1: $M \equiv 0 \pmod{p}$. (Then it is obvious)

Case 2: $M \not\equiv 0 \pmod{p}$, i.e., $p \nmid M$. So $M^{p-1} \equiv 1 \pmod{p}$ by FLT

From $ed \equiv 1 \pmod{(p-1)(q-1)}$ we can write

$ed = k(p-1)(q-1) + 1$ for some $k > 0$

So

$$M^{ed} = M^{k(p-1)(q-1)+1} = (M^{p-1})^{k(q-1)} \cdot M \equiv 1^{k(q-1)} \cdot M \pmod{p}$$

$$\equiv M \pmod{p}$$

□

November 17th

Exercise) Compute the remainder of 29^{196}

Solution:

Let r be the remainder of 29^{196} when divided by 99

Then $0 \le r < 99$ and $r \equiv 29^{196} \pmod{99}$

Since $99 = 9 \cdot 11$, $\gcd(9, 11) = 1$. By SMT, we get

$r \equiv 29^{196} \pmod{9}$ $\quad r \equiv 29^{196} \pmod{11}$ or

$r \equiv 2^{196} \pmod{9}$ $\quad r \equiv (-4)^{196} \pmod{11}$

Since $2^3 \equiv -1 \pmod{9}$, $r \equiv 2^{196} \equiv (2)^{65 \cdot 3 + 1} \equiv -2 \equiv 7 \pmod{9}$

Since 11 is prime, $11 \nmid (-4)$ and $11 \nmid 2$. By FLT, $(-4)^{11} \equiv 1 \pmod{11}$ and $2^{11} \equiv 11 \pmod{11}$

Thus $r \equiv (-4)^{196} = (-4)^{17 \cdot 10 + 6} \equiv ((-4)^{10})^{19} \cdot (-4)^6 \equiv 1^{19} \cdot 4^6 \equiv 2^{12} \equiv 2^{10} \cdot 2^2 \equiv 1 \cdot 4 \equiv 4 \pmod{11}$

We conclude that $r \equiv 7 \pmod{9}$, $r \equiv 4 \pmod{11}$

Since $r = 11k + 4$, $(k \in \mathbb{Z})$, we have $11k + 4 \equiv 7 \pmod{9}$ Note: always start with bigger mod

$\downarrow\ 2k \equiv 3 \pmod 9 \to 8k \equiv 12 \pmod 9 \to (-1)k \equiv 3 \pmod 9 \Rightarrow k \equiv -3 \pmod 9$

Hence $k = 9\ell - 3$ $(\ell \in \mathbb{Z})$, $r = 11k + 4 = 11(9\ell - 3) + 4 = 99\ell - 29$

Hence $r \equiv 70 \pmod{99}$

Complex Number z

in standard form is an expression of the form $z = x + yi$ where $x, y \in \mathbb{R}$

The real number x is called real part of z ($\mathrm{Re}(z)$). The real number y is called the imaginery part of z ($\mathrm{Im}(z)$)

The set is denoted as:

$$\mathbb{C} = \{x + yi,\ x, y \in \mathbb{R}\}$$

The complex numbers $z = x + yi$ and $w = u + vi$ are equal $(z = w)$

$\Leftrightarrow x = u, y = v$

Ex) $z = -1 + \sqrt{2}i$ $\mathrm{Re}(z) = -1$, $\mathrm{Im}(z) = \sqrt{2}$ 2) $z = 7 + (-3)i \to z = 7 - 3i$ $\mathrm{Re}(z) = 7$, $\mathrm{Im}(z) = -3$

$z = 0 + 2i = 2i$ ← purely imaginery $(\mathrm{Re}(z) = 0)$ 4) $z = 5 + 0i \to z = 5$ (real number) (purely real)

↳ $\mathbb{R} \subsetneq \mathbb{C}$

Addition, Multiplication

Let $z = a + bi$, $w = c + di$ be $\mathbb{C}$, then

(+) $z + w = (a + c) + (b + d)i$, $zw = (ac - bd) + (ad + bc)i$ (×)

Note: $i^2 = -1$ and use binomial expansion to calculate a product

Ex) $z = (4 - 3i)(2 + i) \Rightarrow 8 + 4i - 6i - 3i^2 \Rightarrow 8 + 3 - 2i = 11 - 2i$

Additive Identity $\Rightarrow 0 + 0i = 0$ Additive Inverse $\Rightarrow -(x + yi) = -z$ (inverse symbol)

Subtraction identity $\Rightarrow z - w = z + (-w)$ Ex) $(4 - 3i) - (2 - i) = 4 - 3i + (-2 + i) = 2 - 4i$ Subtract $\mathbb{R}$ and $\mathbb{C}$ part

Multiplicative Identity $\Rightarrow 1 + 0i$ Ex) $(x + yi)(1 + 0i) \Rightarrow x + yi$ it's commutative

Multiplicative Inverse

$\forall z \in \mathbb{C}$, the multiplicative Inverse of z exists $\Leftrightarrow z \neq 0$

Moreover, for $z = a + bi \neq 0$, the multiplicative inverse is unique, and

$$z^{-1} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}i = \frac{a - bi}{a^2 + b^2} \quad \text{or} \quad \frac{a - bi}{(a + bi)(a - bi)}$$

Proof:

Existence → Check

$$(a+bi)\left[\frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i\right] = \frac{a^2+b^2}{a^2+b^2} = 1 \quad \Leftarrow \text{Inverse}$$

prove uniqueness

Assume $wz=1$ and $bz=1$ $\quad wz = bz$

then $w^2z = bwz \Rightarrow w=b$

□

Note: $(a+bi)(a-bi) = a^2+b^2$

Devision: $\frac{z}{w} = zw^{-1}$ Ex) $\frac{3-5i}{1+i} \Rightarrow (3-5i)\left(\frac{1-i}{(1+i)(1-i)}\right) = \frac{(3-5i)(1-i)}{(1+i)(1-i)} = \frac{-2-8i}{2} = -1-4i$

November 20th

Boring

Properties of Complex Arithmetic (PCA) *For all $u, v, z \in \mathbb{C}$:*

(1) $(u+v)+z = u+(v+z)$
(2) $u+v = v+u$
(3) $z+0 = z$ *(where $0 = 0+0i$)*
(4) z *has an additive inverse* $-z$ *satisfying* $z+(-z)=0$.
(5) $(uv)z = u(vz)$
(6) $uv = vu$
(7) $z1 = z$ *(where $1 = 1+0i$)*
(8) *If* $z \neq 0$, *then* z *has a multiplicative inverse* z^{-1} *satisfying* $zz^{-1}=1$.
(9) $z(u+v) = zu+zv$.

Proof of 5:

Let $u = a+bi$
$v = c+di$
$z = e+fi$

$\Rightarrow uv = (a+bi)(c+di) = (ac-bd)+(ad+bc)i$

$\Rightarrow (uv)z = [(ac-bd)+(ad+bc)i](e+fi)$
$= [(ac-bd)e - (ad+bc)f] +$
$= [(ac-bd)f + (ad+bc)e]i$
$= [ace-bde-adf-bcf] + [acf-bdf+ade+bce]i$

$\Rightarrow vz = (c+di)(e+fi)$
$= (ce-df)+(cf+de)i$

$\Rightarrow (vz)u = (a+bi)[(ce-df)+(cf+de)i]$
$= [a(ce-df)-b(cf+de)] + [a(cf+de)+b(ce-df)]i$
$= [ace-adf-bcf-bde] + [acf+ade+bce-bdf]i$

Thus, $(uv)z = u(vz)$ □

As usual, we write z^2 for zz, $z^3 = zzz$, etc. If $z \neq 0$, we also use negative integer exponents. All the usual rules of (integer) exponents are true in $\mathbb{C}$ (as they can be deduced from (5) and (8)). But note: we only can raise complex numbers to integer exponents (for now).

Note: $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}_p$ are fields.

Q: Why $\mathbb{Z}_p$ is a field, not $\mathbb{Z}$?

Example) Find a complex number $z = a+i$ satisfying:

$$(1+2i)z^2 + (3-i)z - (\tfrac{3}{4}+i) = 0$$

Solution:

write $z = a+i$, sub it to the equation

1) $z^2 = (a+i)^2 = a^2+2ai+i^2 = a^2+2ai-1 = (a^2-1)+2ai$

2) Sub in

$$(1+2i)(a^2-1-2ai) + (3-i)(a+i) - (\tfrac{3}{4}+i) = (a^2-1-2ai+2a^2i-2-4a) + (3a+3i-ai+1) - (\tfrac{3}{4}+i)$$

$$= (a^2-1-2ai+2a^2i-2-4a+3a+3i-ai+1-\tfrac{3}{4}-i)$$

$$= (a^2-1-4a+3a+1-\tfrac{3}{4}) + [(2a+2(a^2-1)+3-a-1)]i$$

Want $0+0i \Rightarrow$ $= [a^2-a-\tfrac{3}{4}] + [2a^2+a]i = 0$

$a^2-a-\tfrac{3}{4} = 0$ and $2a^2+a = 0$

$a(2a+1) = 0 \leftarrow a = 0, a = -\tfrac{1}{2}$

Since $a=0$ does not satisfy $a^2-a-\tfrac{3}{4}$, but $a=-\tfrac{1}{2}$ is a solution.

Thus, $a=-\tfrac{1}{2}$ is an unique solution and $z = -\tfrac{1}{2}+i$ is the solution.

Challenge: $z = a+\tfrac{2}{5}i$

Definition. Given $z = a + bi \in \mathbb{C}$, the (complex) **conjugate** of z is

$$\bar{z} = a - bi.$$

Examples:

$$\overline{2+3i} = 2-3i$$
$$\overline{-1-i} = -1+i$$
$$\overline{\pi} = \pi$$
$$\overline{i} = -i$$

Properties of Conjugate (PCJ) For all $z, w \in \mathbb{C}$:

(1) $\bar{\bar{z}} = z$
(2) $\overline{z+w} = \bar{z} + \bar{w}$
(3) $z + \bar{z} = 2\,\mathrm{Re}(z)$ and $z - \bar{z} = 2\,\mathrm{Im}(z)i$.
(4) $\overline{zw} = \bar{z}\bar{w}$.
(5) If $z \neq 0$, then $\overline{(z^{-1})} = (\bar{z})^{-1}$.

This is fully proved in the course notes. Let's just prove (3) and (4).
(3) Write $z = a+bi$. Then $z+\bar{z} = (a+bi)+(a-bi) = 2a$ and $z-\bar{z} = (a+bi)-(a-bi) = 2bi$.
(4) Write $z = a+bi$ and $w = c+di$. Then $zw = (ac-bd)+(ad+bc)i$, while

$$\begin{aligned}\bar{z}\bar{w} &= (a-bi)(c-di)\\ &= (ac-bd)+(-ad-bc)i\\ &= \overline{zw}.\end{aligned}$$

□

BTW, we define division $\frac{z}{w} = zw^{-1}$ whenever $w \neq 0$. From (PCJ) we can deduce

$$\overline{\left(\frac{z}{w}\right)} = \overline{zw^{-1}} = \bar{z}\overline{(w^{-1})} = \bar{z}(\bar{w})^{-1} = \frac{\bar{z}}{\bar{w}}.$$

Note that for $z \in \mathbb{C}$ we have the following test for z being "purely real" (in $\mathbb{R}$):

$$z \in \mathbb{R} \iff z = \bar{z}.$$

Can we similarly test for z being "purely imaginary" ($z = bi$, $b \in \mathbb{R}$)?

November 22nd

Definition. Given $z = a + bi \in \mathbb{C}$, the **modulus** of z, written $|z|$, is the non-nonegative real number

$|z| = \sqrt{a^2 + b^2}$ Not absolute value. Not congruence Modulus

Example) $|2+3i| = \sqrt{2^2 + 3^2} = \sqrt{13}$ $\quad |1-i| = \sqrt{1^2 + (-1)^2} = \sqrt{2}$ $\quad |i| = |0+1i| = \sqrt{0+1^2} = 1$

Let $r \in \mathbb{R}$, $|r| = \sqrt{r^2 - 0^2} = \sqrt{r^2} = |r|$ Note, modulus of r = absolute value of r, but can't say AV

Properties of Modulus (PM) *For all $z, w \in \mathbb{C}$:*

(1) $|z| = 0$ *if and only if* $z = 0$.
(2) $|\bar{z}| = |z|$
(3) $\bar{z}z = |z|^2$
(4) $|zw| = |z||w|$
(5) *If* $z \neq 0$, *then* $|z^{-1}| = |z|^{-1}$.

(4) and (5) say that modulus plays nicely with products and inverses. **Warning:** modulus does **not** play nicely with sums.

proof: (3)

Let $z = a+bi$, $\bar{z} = a-bi$, then $z \cdot \bar{z} = (a+bi)(a-bi) = a^2 + b^2 = |z|^2$ as $a^2 + b^2 \geq 0$ □

proof: (4)

if $r, s \in \mathbb{R}$, both non-negative, then $r = s \iff r^2 = s^2$

Let $r = |zw|$, $s = |z||w|$, $r, s \geq 0$, Enough show by (1) $|zw|^2 = (|z||w|)^2$

$|zw|^2 = \overline{zw} \cdot zw$ by (3) $\Rightarrow (\bar{z}\bar{w})(zw)$ (PCJ) $\Rightarrow (\bar{z} \cdot z)(\bar{w} \cdot w)$ (PCA)

↳ $|z|^2 |w|^2$ by (3)

"Coordinate-free proof (no $a+bi$)" □

Example) Prove $\forall z, w \in \mathbb{C}$, $|z+w|^2 + |z-w|^2 = 2(|z|^2 + |w|^2)$

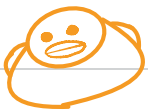
proof:

$|z+w|^2 = \overline{z+w} \cdot z+w$
$= (\bar{z} + \bar{w})(z+w)$
$= (\bar{z})(z) + (\bar{z})(w) + (\bar{w})(z) + (\bar{w})(w)$
$= |z|^2 + (\bar{z})(w) + (\bar{w})(z) + |w|^2$

$|z-w|^2 = (\overline{z-w}) \cdot (z-w)$
$= (\bar{z} - \bar{w}) \cdot (z-w)$
$= (\bar{z})(z) - (\bar{z})(w) - (\bar{w})(z) + \bar{w} \cdot w$
$= |z|^2 - (\bar{z})(w) - (\bar{w})(z) + |w|^2$

$|z+w|^2 + |z-w|^2 = |z|^2 + |w|^2 + |z|^2 + |w|^2 = 2(|z|^2 + |w|^2)$

□



Corollary 5. For all $z_1, \ldots, z_n \in \mathbb{C}$,

(1) $\overline{z_1 + z_2 + \cdots + z_n} = \bar{z}_1 + \bar{z}_2 + \cdots + \bar{z}_n$.

(2) $\overline{z_1 z_2 \cdots z_n} = \bar{z}_1 \bar{z}_2 \cdots \bar{z}_n$.

(3) $|z_1 z_2 \cdots z_n| = |z_1||z_2| \cdots |z_n|$.

Modulus does not play nicely with sums, so we don't get a rule for $|z_1 + z_2 + \cdots + z_n|$. However:

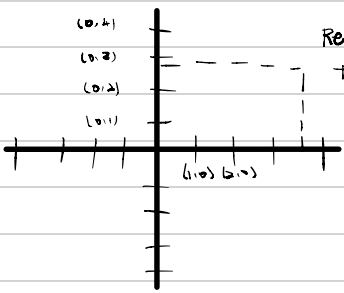
Triangle Inequality (TIQ) *For all $z, w \in \mathbb{C}$,*

$$|z + w| \leq |z| + |w|.$$

To prove this, we need to introduce the **geometry** of $\mathbb{C}$.

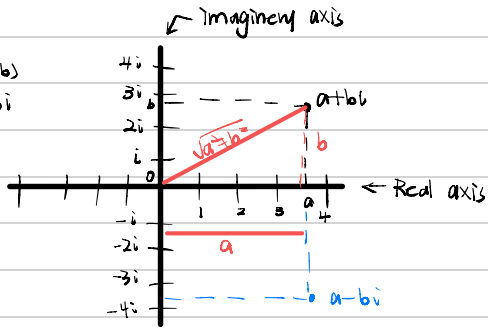
proof:

Cartesian Plan



Replace (a,b) to $z = a + bi$ $\Rightarrow$

Complex Plane / Argand Plane

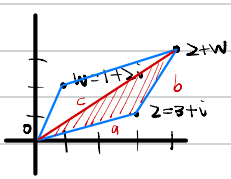


Reintepreting:

Conjugation: if $z = a + bi$, $\bar{z} = a - bi$, then $\bar{z}$ is the reflection of z through the r-axis

Modulus: $|z| = \sqrt{a^2 + b^2}$ = distance from z to 0

Addition:

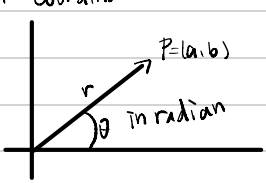


$z + w = 4 + 3i$ $\Rightarrow$ 4th point of the parallelogram whose other points are $0, z, w$

$A = |z|$ $B = |w|$ $C = |z + w|$ $\Rightarrow C \leq A + B \Rightarrow |z + w| \leq |z| + |w|$

Intepreting Multiplication

requires polar coordinate

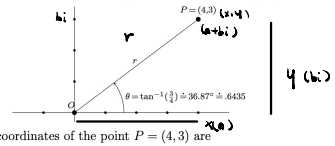


the polar C are (r, θ), $r > 0$

$r = \sqrt{a^2 + b^2}$, $\theta \in \mathbb{R}$ (not determined)

November 24th

Every point $P = (x, y)$ in the plane is described by **polar coordinates** (r, θ) as in the picture:



In the example, the polar coordinates of the point $P = (4, 3)$ are
$(r, \theta) = (5, .6435\ldots)$

Note: all angles are in radian

θ is not unique

↳ replace with θ + 2π ...

$x = r\cos\theta$, $y = r\sin\theta$ $\Rightarrow$ Let $z \in \mathbb{C}$, $z = a + bi$. Let (r, θ) be P.C of (a, b)

↳ $r = |z|$ $\theta =$ "the argument of z" (not angle anymore)

↳ $a = r\cos\theta$, $b = r\sin\theta$ $\Rightarrow z = r\cos\theta + (r\sin\theta)i$

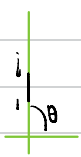
↳ $a + bi = r(\sin\theta + \cos\theta)$

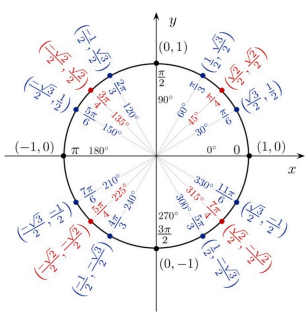
Definition. If $z \in \mathbb{C}$ and the corresponding point has polar coordinates (r, θ), then the expression
$$r(\cos\theta + i\sin\theta)$$
is called a **polar form** for z. Necessarily $r = |z|$. The angle θ is called an **argument** of z.

Example) Find a polar form for $i = 1(\cos\pi/2 + i\sin\pi/2)$

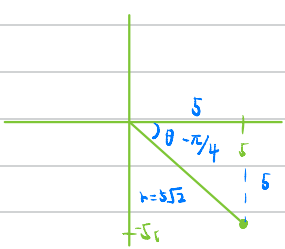
Another polar form: $i = \cos\frac{5\pi}{2} + i\sin\frac{\pi}{2}$)

$0 + 1(i) \rightarrow$ $r = 1$





Example) Find a polar form for $z = 5 - 5i$



Polar form $= 5\sqrt{2}(\cos 7\pi/4 + i\sin(\frac{7\pi}{4}))$

Note: $|z| = \sqrt{(5)^2 - (-5)^2}$

$= \sqrt{50}$

$r = 5\sqrt{2}$

Ex) Write $\cos\frac{15\pi}{6} + i\sin\left(\frac{15\pi}{6}\right)$ in standard form

$\theta = \frac{3\pi}{6} + 2\pi = \pi/2$

$\cos\frac{15\pi}{6} + i\sin\left(\frac{15\pi}{6}\right) = \cos(\pi/2) + (\sin\pi/2)i$

$= i$

Example) Write $-3\sqrt{2} + 3\sqrt{6}i$ in polar form.

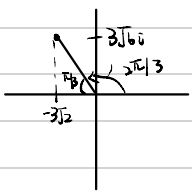
$r = |z|$

$= \sqrt{18 + 54}$

$= \sqrt{72}$

$= 6\sqrt{2}$

$\theta =$



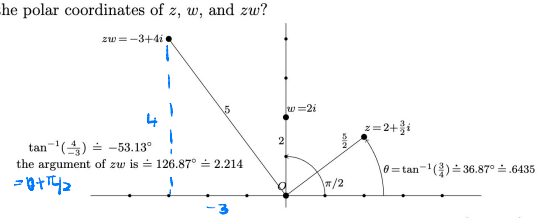
$\Rightarrow z = 6\sqrt{2}\left(\cos\left(\frac{2\pi}{3}\right) + i\left(\sin\left(\frac{2\pi}{3}\right)\right)\right)$

Multiplication of Complex numbers (geometry)

Now consider the product operation. Let $z = 2 + \frac{3}{2}i$ and $w = 2i$. Their product is

$$zw = (2 + \tfrac{3}{2}i)(2i) = -3 + 4i.$$

What about the polar coordinates of z, w, and zw?



In this example, zw is obtained from z and w by **multiplying the moduli** (lengths) and **adding the arguments** (angles). This is true in general.

Polar Multiplication in $\mathbb{C}$ (PMC) *For all $z, w \in \mathbb{C}$, if polar forms for z and w are*

$$z = r(\cos\theta + i\sin\theta)$$
$$w = s(\cos\varphi + i\sin\varphi)$$

then a polar form for zw is

$$zw = rs(\cos(\theta+\varphi) + i\sin(\theta+\varphi)).$$

mult of moduli; add angle

Proof. We just need to prove

$$(\cos\theta + i\sin\theta)(\cos\varphi + i\sin\varphi) = \cos(\theta+\varphi) + i\sin(\theta+\varphi).$$

Well,

$$(\cos\theta + i\sin\theta)(\cos\varphi + i\sin\varphi) = \underbrace{(\cos\theta\cos\varphi - \sin\theta\sin\varphi)}_{\cos(\theta+\varphi)} + \underbrace{(\cos\theta\sin\varphi + \sin\theta\cos\varphi)}_{\sin(\theta+\varphi)}i$$
$$= \cos(\theta+\varphi) + i\sin(\theta+\varphi).$$

Note: special case if $z = r(\cos\theta + i\sin\theta)$, then $z^2 = r^2(\cos 2\theta + i\sin 2\theta)$

$z^3 = r^3(\cos 3\theta + i\sin 3\theta)$

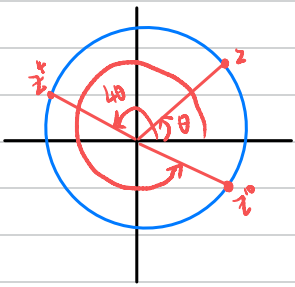
Thus: $z^n = r^n(\cos(n\theta) + i\sin(n\theta))$

De Moivre's Theorem (DMT) *For all $\theta \in \mathbb{R}$ and $n \in \mathbb{Z}$,*

$$(\cos\theta + i\sin\theta)^n = \cos(n\theta) + i\sin(n\theta)$$

November 27th

- $z = \cos\theta + i\sin\theta \Rightarrow |z| = 1$

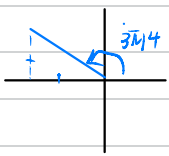


Example) Express $\left(-\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i\right)^{50}$ in standard form

Solution:

Let $z = \frac{-\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$

$|z| = 1 \Rightarrow z = \cos 3\pi/4 + \sin 3\pi/4$



By DMT, $z^{50} = \left(\cos\frac{75\pi}{2} + i\sin\frac{75\pi}{2}\right)$

$= (\cos 3\pi/2 + i\sin 3\pi/2)$

$= 0 + (-i) = -i$

Proof:

For $n>0$, by induction, using (PMC)

Inductive Step:

$(\cos\theta + i\sin\theta)^{k+1} = (\cos\theta + i\sin\theta)^k + (\cos\theta + i\sin\theta)$

$= \cos(k\theta) + i\sin(k\theta) + \cos\theta + i\sin\theta$

$= \cos(k\theta + \theta) + i\sin(k\theta + \theta)$

For $n<0$, Let $n = -m$ $(m>0)$

$(\cos\theta + i\sin\theta)^n = (\cos\theta + i\sin\theta)^{-m}$

$= \frac{1}{(\cos\theta + i\sin\theta)^m}$

$= \frac{1}{(\cos m\theta) + i\sin(m\theta))}$ By DMT.

$= \frac{1}{(\cos(m\theta) + i\sin(m\theta))} \cdot \frac{\cos(m\theta) - i\sin(m\theta)}{\cos(m\theta) - i\sin(m\theta)}$

$(\cos(x)) = (\cos(-x))$, $(\sin(-x)) = -\sin x$

$= \frac{\cos(m\theta) - i\sin(m\theta)}{1}$

$= \cos(n\theta) + i\sin(n\theta)$

For $n=0$, $(\cos\theta + i\sin\theta)^0 = 1 + i0 = 1$

Notation for Complex number $(\cos\theta + i\sin\theta) = \text{cis}\theta$

Example) DMT $\Rightarrow$ $(\text{cis}\theta)^n = \text{cis}(n\theta)$

In polar form: $z = r\cdot(\cos\theta + i\sin\theta) = r\cdot\text{cis}\theta$

PMC $\Rightarrow$ $zw = rs(\text{cis}(\theta+\theta))$

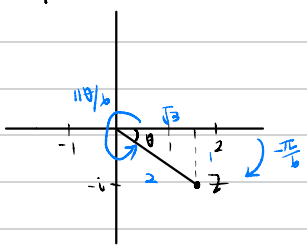
$z = r\text{cis}\theta$

Corollary 9. *For all $z \in \mathbb{C} \setminus \{0\}$ and all $n \in \mathbb{Z}$, if $z = r(\cos\theta + i\sin\theta)$ in polar form, then*
$z^n = r^n(\cos n\theta + i\sin n\theta)$. $z^n = r^n\text{cis}(n\theta)$

Example) Write $(\sqrt{3} - i)^{10}$ in standard form

Solution:

Let $z = \sqrt{3} - i \Rightarrow |z| = 2$



In polar form: $z = 2\,\text{cis}(-\pi/6)$

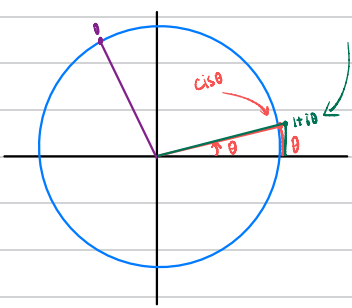
$z^{10} = 2^{10}\,\text{cis}(-10\pi/6)$ or $2^{10}\,\text{cis}(-5\pi/3)$

$z^{10} = 2^{10}\,\text{cis}(\pi/3)$

$z^{10} = 1024\,(\frac{1}{2} + i\frac{\sqrt{3}}{2})$

$z^{10} = 512 + (512\sqrt{3})i$

Example) Solve $z^6 = -64$



For any θ, very large n,

$\cos\theta/n + i\sin\theta/n \approx 1 + \theta/n$

Raise to n^{th} power, $\cos\theta + i\sin\theta \approx (1 + \theta i/n)^n$

$$\cos\theta + i\sin\theta = \lim_{n\to\infty}(1 + \theta i/n)^n$$

Notice: $\lim_{n\to\infty}(1 + 1/n)^n = e$ $\quad \lim_{n\to\infty}(1 + \frac{x}{n}) = e^x$

then $\cos\theta + i\sin\theta = e^{i\theta}$

Let $\theta = \pi$, then $\cos\pi + i\sin\pi = e^{i\pi} = -1$

November 29th

Ex) Solve $z^6 = -64$

Solution:

In polar form: $z = r\text{cis}\theta \Rightarrow z^6 = r^6\text{cis}(6\theta) \Rightarrow r^6 \cdot \text{cis}(6\theta) = 64\,\text{cis}(\pi)$ ①

$-64 = 64 \cdot \text{cis}(\pi)$

Solve ①: $r^6 = 64$. $\Rightarrow r = 2 \; (r \geq 0)$

$6\theta = \pi$ or 3π or 5π ..... $\theta = \frac{\pi + 2k\pi}{6}$ $(k \in \mathbb{Z})$

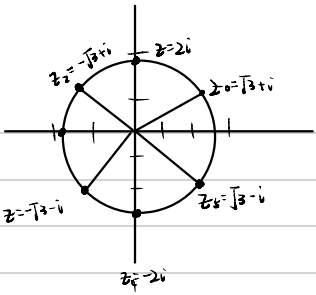
$= \pi + 2k\pi \; (k \in \mathbb{Z})$

Let $\theta_0 = \frac{\pi}{6}$

$z_0 = 2\,\text{cis}\frac{\pi}{6} = 2(\cos\pi/6 + i\sin\pi/6)$

$= 2(\frac{\sqrt{3}}{2} + i\frac{1}{2})$

$= \sqrt{3} + i$



Let $k=1$, $\theta_1 = \pi/2 \Rightarrow z_1 = 2\text{cis}(\frac{\pi}{2}) = 2i$

Let $k=2$, $\theta_2 = 5\pi/6 \Rightarrow z_2 = 2\text{cis}(\frac{5\pi}{6}) = -\sqrt{3}+i$

Let $k=3$, $\theta_3 = 7\pi/6 \Rightarrow z_3 = 2\text{cis}(\frac{7\pi}{6}) = -\sqrt{3}-i$

$\therefore z_0 \to z_5$ are 6 solutions to $z^6 = 64$

↳ called Complex 6 roots of -64

Definition. Given nonzero complex number $a \in \mathbb{C}$ and $n \in \mathbb{N}$, the complex number(s) $z \in \mathbb{C}$ satisfying $z^n = a$ are called the **complex n-th roots** of a.

Complex n-th Roots Theorem (CNRT) *For all complex numbers $a \in \mathbb{C}$, if $a \neq 0$ and in polar form*

$$a = r(\cos\theta + i\sin\theta),$$

then a has exactly n complex n-th roots given by

$$z = \sqrt[n]{r}\left(\cos\left(\frac{\theta+2k\pi}{n}\right) + i\sin\left(\frac{\theta+2k\pi}{n}\right)\right), \quad k = 0, 1, 2, \ldots, n-1.$$

Solutions: Complex n^{th} root(s) of a

Example) Find cube roots of i

Solution:

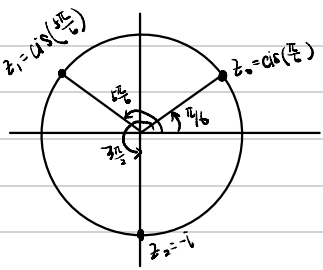
Let $i = \text{cis}(\frac{\pi}{2})$

By CNRT, $z = \sqrt[3]{1}\,\text{cis}\left(\frac{\frac{\pi}{2}+2k\pi}{3}\right)$ $(k=0,1,2)$

↳ $k=0 \Rightarrow z_0 = \text{cis}\,\pi/6 \Rightarrow \sqrt{3}/2 + 1/2\,i$

↳ $k=1 \Rightarrow z_1 = \text{cis}\,5\pi/6$

↳ $k=2 \Rightarrow z_2 = \text{cis}(3\pi/2)$



Proposition 11 (Quadratic Formula) *For all complex numbers $a, b, c \in \mathbb{C}$ with $a \neq 0$, the complex solutions to*

$$az^2 + bz + c = 0$$

are given by

$$z = \frac{-b \pm w}{2a}$$

where $\pm w$ are the two complex square roots of $b^2 - 4ac$.

This isn't always useful when looking for exact answers.

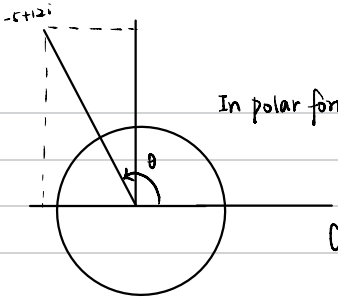
Ex) Solve $z^2 - 2z + b = 12i$

Solution: $z^2 - 2z + (6-12i) = 0 \Rightarrow a=1,\ b=-2,\ c = 6-12i$

Using Quadratic Formula: $z = \frac{2 \pm w}{2}$ where $w = 4 - 4(6-12i)$

$= 4 - 24 + 48i$

$= -20 + 48i$



In polar form: $-5+12i = 13\,\mathrm{cis}\,\theta$ $\quad \theta \doteq 1.966$

Square roots: $z_0 = \sqrt{13}\cdot \mathrm{cis}(\theta/2) = (1.99, 2.99)$

$z_1 = \sqrt{13}\cdot \mathrm{cis}\left(\frac{\theta+2\pi}{2}\right) = -z_0$

Could the exact value of z_0 be $2+3i$

$(2+3i) = -5+12i \Rightarrow z_0 = 2+3i$ is $\sqrt{}$ of $-5+12i$

↳ $w = 4+6i$ is a $\sqrt{}$ of $-20+48i$

∴ Solutions are: $z = 2 \pm (4+6i)/2$

$= 3+3i,\ -1+3i$

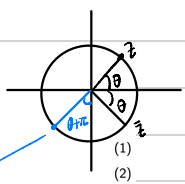
December 1st

Two final notes about polar form:

If $z = r\,\mathrm{cis}\,\theta$, then

$\bar{z} = r\,\mathrm{cis}(-\theta)$ (1)

$-z = r\,\mathrm{cis}(\theta+\pi)$ (2)



Application: Solve $z^4 + 4\bar{z} = 0$.

Solution: write

$$z = r\,\mathrm{cis}\,\theta.$$

Rewrite the equation as $z^4 = -4\bar{z}$

In polar form, this becomes $r^4\mathrm{cis}(4\theta) = -4r\mathrm{cis}(-\theta)$ (need non-negative)

Thus ↳ $r^4\mathrm{cis}(4\theta) = 4r\mathrm{cis}(\pi-\theta)$

$\therefore r^4 = 4r$, $4\theta = \pi - \theta + 2k\pi$ ($k \in \mathbb{Z}$)

---

§10.7

Definition

A **polynomial in x over $\mathbb{R}$** is an expression of the form

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x + a_0$$

where the **coefficients** $a_0, a_1, \ldots, a_n$ are in $\mathbb{R}$.

Can also have polynomials **in** $y, z, t, \ldots$

Can also have a polynomial **over** $\mathbb{C}$ ($a_0, \ldots, a_n \in \mathbb{C}$).

Examples

- $2x^2 - \frac{\pi}{2}x + \sqrt{17}$ (in x over $\mathbb{R}$ / $\mathbb{C}$)
- $3z^4 - (2+i)z^2 + 3z - i$ in z over $\mathbb{C}$
- $3x + \sqrt{2x}$ not polynomial
- $z^4 + 4\bar{z} + (1+i)$ not a polynomial (no conjugate (not a power of z))

Definition

Given a polynomial

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

- Each a_i is a **coefficient**.
- Each $a_i x^i$ is a **term**.
- Assume $a_n \neq 0$. Then:
  - a_n is the **leading coefficient**;
  - $a_n x^n$ is the **leading term**;
  - n is the **degree** of the polynomial.
- 0 is the **zero polynomial**. Its degree is undefined.
- A polynomial is:
  - **constant** if its degree is 0, or it is the zero polynomial. a_0
  - **linear** if its degree is 1. $a_1 x + a_0,\ a_1 \neq 0$
  - **quadratic** if its degree is 2. $a_2 x^2 + a_1 x + a_0,\ a_2 \neq 0$

(leading coe. of 0 degree $\frac{1}{2}(a_0)$)

$\mathbb{R}[x]$ – the set of all polynomials in x over $\mathbb{R}$.

$\mathbb{C}[z]$ – the set of all polynomials in z over $\mathbb{C}$.

We can add, subtract, multiply polynomials (in the same variable).

In this way, the sets $\mathbb{R}[x]$ and $\mathbb{C}[z]$ are "similar to" the set of integers.

Definition

For $f(x), g(x) \in \mathbb{R}[x]$, we say that $g(x)$ **divides** $f(x)$, and write

$$g(x) \mid f(x)$$

if there exists $h(x) \in \mathbb{R}[x]$ such that $f(x) = g(x)h(x)$.

Similarly for $f(z), g(z) \in \mathbb{C}[z]$. (Allowing $h(z) \in \mathbb{C}[z]$)

Ex) $x+1 \mid x^2-1 \Rightarrow (x-1)(x+1) = x^2-1 \Rightarrow$ true

Ex) $\sqrt{5}x^5 - 27x^4 + ix - (1+i)$

(leading coe. ↖, degree ↗)

How to tell if $f(x) \mid g(x)$? Long Division of Polynomials.

Example 17: test whether $(x^2+1) \mid (3x^4+x^3-4x^2+x-7)$ $\Rightarrow$ $3x^4+x^3-4x^2+x-7 = (x^2+1)(3x^2+x-7)$

Solution

$$
\begin{array}{r}
3x^2+x-7 \\
x^2+1 \;\overline{)\; 3x^4+x^3-4x^2+x-7} \\
3x^4+0+3x^2 \\
\hline
x^3-7x^2+x \\
x^3+0+x \\
\hline
-7x^2-7 \\
-7x^2-7 \\
\hline
0
\end{array}
$$

Everything we did (starting in §3.4) for $\mathbb{Z}$, we can do for $\mathbb{R}[x]$ or $\mathbb{C}[z]$:

- (TD)
- (DIC)
- Division Algorithm
- GCDs
- Euclidean Algorithm
- Bézout's Lemma
- (CCT)

"Primes," and "prime" factorizations of polynomials, are a little different.

In addition, polynomials are also functions, and we can ask for solutions in $\mathbb{R}$ (or in $\mathbb{C}$) to polyomial equations

$$f(x) = 0.$$

Factorizations and solving equations are related.

Let $f(x) \in \mathbb{R}[x]$ or $\mathbb{C}[x]$.

An element $c \in \mathbb{R}$ (or $\in \mathbb{C}$) is a **root** of $f(x)$ if it solves $f(x) = 0$.

Solution(

Factor Theorem (FT) for $\mathbb{R}[x]$

For all $f(x) \in \mathbb{R}[x]$ and $c \in \mathbb{R}$,

$$f(c) = 0 \iff (x-c) \mid f(x).$$

Factor Theorem (FT) for $\mathbb{C}[z]$

For all $f(z) \in \mathbb{C}[z]$ and $c \in \mathbb{C}$,

$$f(c) = 0 \iff (z-c) \mid f(z).$$

Example: $f(z) := z^4 - 1$.

The roots of z^4-1 are the solutions to

$$z^4 - 1 = 0 \quad \text{i.e.,} \quad z^4 = 1,$$

which are the complex 4th-roots of 1.

One complex 4th root of 1 is i.

Thus by (FT) for $\mathbb{C}[z]$,

$$(z-i) \mid (z^4-1).$$

We could do the long division to find

$$z^4 - 1 = (z-i)(z^3+iz^2-z-i)$$

In fact, z^4-1 completely factors as

$$z^4 - 1 = (z^2+1)(z^2-1) = (z+i)(z-i)(z+1)(z-1)$$

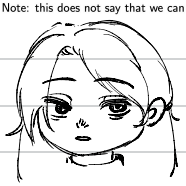
This generalizes.

Complex Polynomials of Degree n Have n Roots (CPN)

For every $f(z) \in \mathbb{C}[z]$ with $\deg f(z) = n \geq 1$ and leading coefficient a_n, there exist $c_1, \ldots, c_n \in \mathbb{C}$ such that

1. $f(z)$ factors in $\mathbb{C}[z]$ as
$$f(z) = a_n(z-c_1)(z-c_2)\cdots(z-c_n)$$
2. The roots in $\mathbb{C}$ of $f(z)$ are exactly $c_1, c_2, \ldots, c_n$ (possibly some of these are repeated).

Note: this does not say that we can **find** $c_1, \ldots, c_n$.



We won't prove (CPN) (or anything in this section).

But the main idea is to argue by induction on n.

In the inductive step, it is enough to find **one** root; then apply (FT).

So the main difficulty is in proving

Fundamental Theorem of Algebra (FTA)

Every $f(z) \in \mathbb{C}[z]$ with $\deg f(z) \geq 1$ has a root in $\mathbb{C}$.

Every ① Degree complex number polynomial has a root in complex number

(FTA) is a classical and very deep theorem about the complex numbers.

When I was first hired 30 years ago, we sketched the proof in MATH 135.

- Now, search for a proof on YouTube.

What about factoring polynomials $f(x) \in \mathbb{R}[x]$?

- They are in $\mathbb{C}[x]$, so (CPN) applies.
- But what if we only want factors in $\mathbb{R}[x]$?

Real Factors of Real Polynomials (RFRP)

Every $f(x) \in \mathbb{R}[x]$ of degree ≥ 1 can be written as a product of real linear and real quadratic factors.

Example:

$x^4 + x^3 - 2x^2 - 3x - 3 =$

(Over $\mathbb{C}$: $=$

December 4th

Complex Polynomials of Degree n Have n Roots (CPN). *Every $f(z) \in \mathbb{C}[z]$ with $\deg f(z) = n \geq 1$ factors in $\mathbb{C}[z]$ as*

$$f(z) = a_n(z - c_1)(z - c_n)\cdots(z - c_n).$$ (linear) Factorization of f(z)

Obviously the linear factors $z - c_i$ cannot be further factored. We say they are **irreducible** in $\mathbb{C}[z]$. $(z-c)$

Example) Factor z^4+9 into irreducible factor in $\mathbb{C}[z]$

Solution:

Roots of $z^4+9 \Leftrightarrow$ to $z^4 = -9 \Rightarrow$ complex 4th roots of -9

① Rewrite as polar form:

$-9 = 9\,cis(\pi)$

② By CNRT, the roots are $\sqrt[4]{9}\,cis\left(\frac{\pi+2k\pi}{4}\right)$, $k=0,1,2,3$.

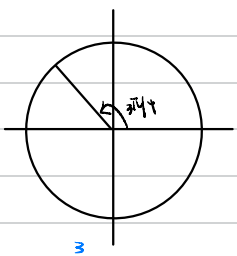
③ Find:

$k=0$, $\sqrt{3}\cdot cis\left(\frac{\pi}{4}\right) = \sqrt{3}\left(\frac{\sqrt{2}}{2}+\frac{\sqrt{2}}{2}i\right) = \frac{\sqrt{6}}{2}+\frac{\sqrt{6}}{2}i$

$k=1$, $\sqrt{3}\,cis\left(\frac{3\pi}{4}\right) = \sqrt{3}\left(\frac{-\sqrt{2}}{2}+\frac{\sqrt{2}}{2}i\right) = \frac{-\sqrt{6}}{2}+\frac{\sqrt{6}}{2}i$

$k=2$, $\sqrt{3}\,cis\left(\frac{5\pi}{4}\right) = \frac{-\sqrt{6}}{2}-\frac{\sqrt{6}}{2}i$

$k=3$, $\sqrt{3}\cdot cis\left(\frac{7\pi}{4}\right) = \frac{\sqrt{6}}{2}-\frac{\sqrt{6}}{2}i$



④ Factorization: $z^4+9 = \left(z-\left(\frac{\sqrt{6}}{2}+\frac{\sqrt{6}}{2}i\right)\right)\left(z-\left(\frac{-\sqrt{6}}{2}+\frac{\sqrt{6}}{2}i\right)\right)\left(z-\left(\frac{-\sqrt{6}}{2}-\frac{\sqrt{6}}{2}i\right)\right)\left(z-\left(\frac{\sqrt{6}}{2}-\frac{\sqrt{6}}{2}i\right)\right)$

Example) Factor x^4+9 into a product of irreducible factors in $\mathbb{R}[x]$.

Trick: Factor in $\mathbb{C}[x]$, Pair together linear (complex) factors corresponding to conjugate pairs of roots.

Notice: for ④, 1, 4 are conjugate, 2, 3 are conjugate.

Solution: 1-4.

$$(z-c_1)(z-c_4) = (z-c_1)(z-\bar{c}_1) = z^2-(c_1+\bar{c}_1)z+c_1\bar{c}_1 = z^2-2Re(c_1)z+|c_1|^2$$

$$= z^2-\sqrt{6}z+3$$

Similarly: $(x-c_2)(x-c_3) = x^2+\sqrt{6}x+3$

Thus, $x^4+9 = (x^2-\sqrt{6}x+3)(x^2+\sqrt{6}x+3)$ ⇐ Irreducible factors in $\mathbb{R}[x]$

only works when 2 roots conjugate.

Lemma 17. *For all $c \in \mathbb{C}$, $(x-c)(x-\bar{c}) \in \mathbb{R}[x]$.*

Conjugate Roots Theorem (CJRT). *For all $f(x) \in \mathbb{R}[x]$, if $c \in \mathbb{C}$ is a root $f(x)$, then so is $\bar{c}$*

if $f(c)=0$, then $f(\bar{c})=0$

Proof: (CJRT)

Conjugate plays nicely with everything, Conjugate of $\mathrm{Re}(z) = \mathrm{Re}(z)$

Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ with $a_0, a_1, \dots a_n \in \mathbb{R}$

Since $f(c) = 0$, that means $0 = a_n c^n + a_{n-1} c^{n-1} \dots + a_1 c + a_0$ (c is a root)

take conjugate of both sides: $\overline{0} = \overline{f(c)} = \overline{a_n c^n} + \overline{a_{n-1} c^{n-1}} \dots \overline{a_1 c_1} + \overline{a_0}$

$= \overline{a_n} \cdot \overline{c^n} + \overline{a_{n-1}} \cdot \overline{c^{n-1}} \dots \overline{a_1} \cdot \overline{c_1} + \overline{a_0}$ ($\overline{c^n} = (\overline{c})^n$)

$= a_n (\overline{c})^n + a_{n-1} (\overline{c})^{n-1} \dots a_1 \cdot \overline{c_1} \cdot a_0$ (By Property $\overline{a} = a$)

$\therefore f(\overline{c}) = 0$

∎.

Example) $f(x) = x^4 - 5x^3 + 16x^2 - 9x - 13$

① Factor into irreducible (linear / quadratic) in $\mathbb{C}[x]$

② Factor into same thing in $\mathbb{R}[x]$

Hint: $2-3i$ is a root.

Solution:

By CJRT, $2+3i$ is also a root. So $(x-(2-3i))(x-(2+3i))$ is a factor.

$= (x^2 - 4x + 13)$

Then, By long divisions: $x^2 - 4x + 13 \;)\; x^4 - 5x^3 + 16x^2 - 9x - 13$ $\quad x^2 - x - 1$

$x^4 - 4x^3 + 13x^2$

$-x^3 + 3x^2 - 9x$

$-x^3 + 4x^2 - 13x$

$-x^2 + 4x - 13$

$-x^2 + 4x - 13$

0

$\therefore f(x) = (x^2 - 4x + 13)(x^2 - x - 1)$ $\quad x = \frac{1 \pm \sqrt{5}}{2}$ $\quad \Rightarrow (x^2 - 4x + 13)\left(x - \frac{1+\sqrt{5}}{2}\right)\left(x - \frac{1-\sqrt{5}}{2}\right)$

↑ irreducible in $\mathbb{R}[x]$

END!!!